International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

ELECTRONIC BANKING AND SECURITY THREATS

Sali Bakare*

University of the People, Business Administration Division

ABSTRACT

The banking industry has witnessed great changes in the last twenty years. Some of these changes include mergers, the growth of electronic banking, and consolidation of banks with other financial institutions such as insurance companies and investment banking firms. These changes have some positive impacts on banks' profitability, increased public's access to diverse financial services, and facilitated bank lending. Electronic banking (E-banking/EB) is becoming increasingly popular because it simplifies and speeds transactions. E-banking enables customers to bank conveniently at the corner of their homes and enhances profitability and productivity for banks. Although e-banking provided some benefits to the banks and their customers, it also brought along with it some security threats.

Keywords: Electronic banking; Information technology; Innovation; Cyber crime, E-banking security threat, Phishing Scam, Online fraudsters, E-banking

INTRODUCTION

The banking industry has undergone significant changes with the introduction of information technology (IT). IT has altered the delivery of banking products and services globally [2]. As noted by [2], the banking industry operating in a complex and competitive environment has become aware of the need to serve its customers electronically.

For the banking industry, competition is intense, business environment is challenging, and economic growth is slow [8]. [20] noted that investments in technology as well as the population are increasing, while economic growth is at a stand still. The US banking industry is therefore; taking steps to improve its profitability and competitiveness via product redesigning, cost restructuring, and mergers and acquisitions to help failing banks.

Because financial institutions only provide simple security measures such as username and password for their customers to conduct online transactions, it is easy for fraudsters to

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

compromise these simple security mechanisms. It is therefore, crucial that financial institutions upgrade their security systems.

ELECTRONIC BANKING

Electronic banking is the act of delivering bank products and services via electronic communication network to bank customers [6]. E-banking enables customers to conduct a range of financial transactions through the financial institution's website or telephone system. E-banking is becoming increasingly popular as it brings convenience, simplicity, and speed to users [5]. E-banking has become the preferred way for many Americans to conduct financial activities. For most people in the United States and Europe, e-banking means 24hours a day access to cash via ATM. The three main delivery channels in e-banking are: ATM's, telephone-banking, and internet banking. It is critical for banks to provide e-banking services effectively and efficiently. Banks therefore, need to ensure there are enough e-banking customers to justify the provision of e-banking services. Otherwise, banks' profitability and sustainability might be at stake.

Electronic banking enables users to conveniently manage their finances anytime, anywhere; however, online transactions can be vulnerable to security threats. Some financial institutions only provide simple authentications such as username and password to conduct online transactions. These simple authentications can easily be compromised by fraudsters. Financial institutions and bank regulators are therefore, upgrading from a single authentication to advanced security mechanism including using a one-time password.

Types of Electronic Banking

Some types of electronic banking services available are telephone banking, internet banking, and automated teller machine (ATM).

Automatic Teller Machine (ATM)

An ATM is a 24/7 electronic terminal that allows customers to bank with convenience [3]. Automated teller machines are located outside of banks, at airports, malls, and sometimes, away from customers' home banks. Customers sometimes may have to pay a fee if the ATM is located away from their banks; the amount depends on individual banks. Automated teller machines enable a customer to deposit or withdraw cash with the use of a card and a personal identification number (PIN) at any time from his/her account; the transaction is then credited or debited accordingly. Automated teller machines have increased bank productivity and saved customers time as opposed to queuing in bank halls. Customers can utilize the time saved on other productive activities.

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

Telephone banking

Telephone banking (TB) enables customers to perform financial transactions over the phone. Most financial institutions in the US offer the service on a 24/7 basis. [18] noted that to use a financial institution's telephone banking service, a customer has to register with the institution for the service; set up a password, and call a special phone number provided by the financial institution to access the service. Telephone banking brings banking to the customers' doorsteps and is done through Interactive Voice Response (IVR) system ([7] as cited by [1]). Telephone banking provides customers with increased convenience, expanded access, and significant time saving; while it reduces operational cost for banks [1]. Bank customers can inquire about account balance, interest rates, foreign exchange rates, account statements, request for check books; transfer funds, pay bills, stop payment, and check balances with their (mobile) phones [18].

Internet Banking

The Internet is vastly becoming an important distribution channel for many businesses including banks. Internet banking is another imminent step in the e-banking evolutionary process as it is now one the effective and efficient delivery channels of e-banking. [17] stated that most banks that embark on internet banking did so to (a) create new opportunities for the bank, b) enable the bank to be competitors and c) reduce costs. Internet banking is now a strategic necessity as it brings banks higher profitability [17]. Online banking becomes an avenue for banks to reduce costs; which banks in turn pass to their customers in the form of lower service fees [20]. Customers enjoy the ease and convenience of banking at home at their own time while they experience an improved access to financial statement. [17] noted that the increasing rate of personal computer sales show great prospects in the future use of Internet banking in the US.

Challenges of Electronic Banking to Banks

The main challenges of e-banking are inadequate infrastructure, unexpected system failure, cyber security threats [18], and unreliable power failure (in developing countries). Unlike in most third world countries, power failure and Internet connectivity are not much of a problem in the United States and Europe. Privacy and security issues, cyber fraud, phishing scam, Internet account hacking may pose a major concern to a lot of bank customers around the globe. Good Internet connectivity, reliable electricity, reliable privacy and security are critical to the success of electronic-banking. Lack of specific laws to govern Internet banking is another important concern for banks and their customers.

Impacts of E-banking

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

[5] and [18] indicated in their study findings that e-banking helped banks to reduce operational costs. [15] revealed that e-banking has enhanced and increased bank productivity; and that it has a positive impact on bank revenue. [15] indicated that there is a significant and positive correlation between IT and bank performance. These researchers also noted that bank growth improved and bank efficiency was enhanced due to e-banking. Banks are intermediaries between the sources and uses of funds; this service improves economic growth. As e-banking helps to enhance bank efficiency, it also helps to increase the speed at which banks help to improve economic growth.

Security Threats

The banking industry is the most sensitive industry in terms of online security [11]. In the last two decades, as e-banking services grew in popularity, so did security threat and cyber crime. Although e-banking brings opportunities and benefits to banks and their customers, it also involves risks that need to be addressed by bank management and bank regulatory and supervisory authorities. E-banking increases security risks because it exposes users' information to risky environment [19]. As noted by [19], security breaches can be categorized into three: a). flaws in system design that can lead to breaches, b). breaches by casual hackers, and c). breaches with serious criminal intent.

Flaws in the System

In 2011, mobile banking rose 63%; and security threats are constantly evolving [21]. Smart phones and the Internet have security flaws. As mobile banking usage is increasing; mobile security is becoming increasingly challenging because the measures which the financial institutions have to control online banking threats do not seem to work well with mobile devices. Most mobile banking applications suffer from security flaws.

In the US, Bank of America (BOA) exposed customers' account data in 2011 due to a Website oversight [12]. In 2014, a security expert noted that with reverse engineer, it is possible to compromise bank apps; and that two-faction authentication cannot prevent the tampering. In 2014, Kickstarter's, Target's, eBay's, and AT&T's databases were hacked.

United States Computer Emergency Readiness Team (US-CERT) indicated in its study result that most mobile applications lack valid secure socket layer (SSL) certificates. Secure socket layer certificate is a major mechanism that banks use to protect their customers against security threats. Sixty-eight percent of the applications on Google Play do not check server certificates; while 77% ignore SSL errors [16].

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

The issue of confidentiality and integrity has become a concern for many banks. Bank fraud is more challenging for countries with less sophisticated security infrastructure [4]. Malicious applications that steal financial account information have increased dramatically over the last few years [22].

Breaches by Casual Hackers

As noted by [4], online banking fraud is a global phenomenon that is constantly evolving. Online banking security has become a necessity because of the increasing cyber crimes. It is crucial to understand how cyber criminals threaten security.

The greatest threat to e-banking security is the malware-based attacks [16]. With malware, attackers compromise codes in the browser; this enables an attacker to modify banking transaction contents and then use customers' information and identities to secretly complete transactions without customers' consent. Another tool the attackers use is the fake distributed denial-of-service (DDoS). Hackers use a server-hosted kit to inject malicious codes onto banks' Websites. When a customer visits the Website, the code compromises his or her personal computer (PC) to gain control over the PC.

Hackers may use compromised machines to make banks' sites unavailable to customers. Hackers also use Trojan, which is capable of stealing account information by tricking people into fake bank Websites. Trojan is able to steal any information entered unto a web page before it is encrypted by secure sockets layer (SSL), which is the standard security technology used by financial institutions for establishing an encrypted link between a web server and a browser. Trojan is capable of bypassing desktop firewalls when making outgoing connections [22]. Trojan is also capable of generating a pop-up window that contains a carbon copy of the original service Website. Any information entered into this pop-up window is prone to security threat. Because SSL cannot protect bank customers from visiting fake Websites, it is possible for hackers to decrypt and re-encrypt traffic and then forward it to banks' Websites. However, [16] noted that if people refrain from opening unsolicited emails and banks update their software periodically, online banking security threats would be reduced greatly.

Breaches with Serious Criminal Intent

Fraudsters can install software called keylogger on a computer, which a bank customer uses to log in to his or her account. Keylogger captures sensitive information which the fraudster can later use for fraudulent acts. Spyware is another software that is used to secretively collect user information while the user is on the Internet. Another way of scheming users is phishing. This is where fraudsters send malicious emails out to bank customers and impersonate financial

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

institutions. If and when attackers cannot gain access, they will often organize a denial of service attack.

In 2010, some phishing schemes were targeted at military account holders and World Bank officials. Phishing attacks rank No. 3 among fraud threats [13]. Unsecured Wifi is a free and easy way for fraudsters to gain access to users' information.

Consumers' risky behavior makes them prone to attacks from fraudsters. For instance, a skimmer may insert skimming device in the ATM machine and sticks around. When a bank customer comes and inserts his or her debit card, the card will get stuck in the ATM machine. The skimmer will then come out like an innocent helper and suggests the customer re-enters his or her PIN. Once the customer did, the skimmer has the information and the card. While the customer goes to report the incident or make a phone call, the skimmer will remove the skimming device and the card and then flee. Over the years, the skimmers' ability to turn stolen data into cash increases, while their chances of getting caught decrease [13].

In the US, skimmers use magnetic stripe system. This system, according to experts is easier for the fraudsters than the other skimming devices. They can go to retail places and swap the point of sale (POS) device with a fake one. Banks therefore, need to implement stronger cardholder authentication; which may require changing their infrastructure.

Fraud threats have increased as new threats and channels blossom daily. In 2010, automated clearing house (ACH) fraud, which resulted in corporate account takeover increased significantly [13]. Mobile malware and Zeus attacks are two of the emerging threats. Banks should therefore, not leverage current online banking security infrastructure to avoid high risk.

Internal Threat

There is internal threat of data leakage. Sometimes financial institutions' employees intentionally or accidentally expose sensitive information for instance on social media or if an when an employee walks away from his or her desk without closing the computer screen. Malicious attacks may be staged by aggrieved employees within an organization [13]. Internal fraud is one of the biggest issues in financial services [13]. To mitigate internal risks of data leakage, organizations must have social networking policies in place and educate employees.

Impacts of Security Threat

Attacks are getting more sophisticated; this makes stronger authentication a necessity [13]. Credit card losses in 2004 were about $1.8 billion; while debit card losses were $810 million. In

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

2007, credit card losses increased to $2.04 billion and debit card losses rose to $1.05 billion. According to the FBI report (as cited by [13]), Zeus was linked to about $100 million financial losses worldwide in 2011 alone. In 2010, commercial banks came up with desktop hardening and anti-Trojan services to curb online banking threats. Some banks such as Bank of America are educating their customers on how to prevent fraud.

In 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a supplemental guidance to enhance the authentication of Internet banking environment. Some banks have introduced better security methods such as the public key infrastructure (PKI) smartcards; however new transaction methods should still be introduced. Software designed to identify risk levels and help financial institutions to assign controls in mitigating cyber security risk is now available in the market. In this software, a tool designed to educate financial institutions' customers in security awareness is included [12].

There is a notion that the phishing schemes are coming from Russia. The manufacturers and distributors of ATM skimming devices are in Eastern Europe and the Middle East [13]. And because of differences in international laws and enforcement policies, it is difficult to bring justice to the phishing skimmers. For instance, in Eastern Europe, it is not a crime to sell a hacking code; and there are no laws against cyber crime. [10] quoted Neil Schwartzman, a senior security-standards director at Return Path Inc., an e-mail deliverability company, as saying "cyber crime is a war that is becoming a crisis". [10] noted that it is easy for international cyber criminals to transfer dollars from US commercial accounts to Eastern Europe; and that this is a national security issue, which requires government attention.

Recommendations for Banks

The banking industry should launch a global effort to fight phishing schemes. Banks should (a). educate customers and members so they are aware of how institutions will communicate information. Banks should authenticate all the e-mails they send out to customers. This way, bank customers will not be victims to fraudsters. (b). invest in consumer-quality technology that will alert customers when their balances fall below certain levels, (c). monitor transaction history; so, when the bank notices repetitive testing of code combinations for a transaction, it will be treated as a red flag. (d). authenticate the card CV value on ATM and POS transactions; so if and when phishers steal card information, they will not be able to conduct a transaction. Some banks and credit unions usually will call their business customers for every ACH file that is submitted. Bank of America (BOA) holds educational Webinars to educate their business customers on existing and emerging threats to electronic banking and the steps that customers can take to help prevent fraud. Banks should regularly proactively test their security systems

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

control to ensue customers' information is secure. Banks should maintain sufficient staff with information security expertise. Supervisors should stay on top of information security.

[13] noted that bank regulators need to start enforcing the FFIEC guidance and banks need to upgrade their security systems. However, it is challenging for banks to identify which technologies or parts of their infrastructure to upgrade. Banks need to take action against cyber crime so that customers will not lose confidence in online banking. Because e-banking is reducing overall costs for banks, banks should invest in technologies that will enhance online security for them (banks) and their customers in order for them to continue enjoying the benefits of e-banking.

Recommendations for Customers

For safety, bank customers should avoid using the same login information on all their online accounts. Online banking users should not use public Wifi for their banking transactions. To avoid the risk of unauthorized persons gaining access to their data, online banking customers should have anti-virus protection on their devices to enhance security. Some systems and applications are vulnerable to security threat risks; and banks do not have control over these systems. Therefore, bank customers should be selective of the applications and systems they use. Online banking users should endeavor to change their passwords regularly and log off when they finish a session online. Banks encourage customers to back up files by saving them unto removable drives such CDs or thumb drives and check their accounts on a regular basis. When customers suspect fraud, they should report to their banks immediately.

General Safety Measures

Financial services customers should use a strong password consisting of six to eight characters long and a combination of upper and lower-case letters, numbers, and special symbols. Customers should avoid using dates of birth as their passwords. They should not download any applications from unreliable sources to avoid viruses or Trojan horses. Bank customers should not open an attachment if they do not know or trust who sent it. Customers must use an up-to-date operating system to ensure no security loop holes exist. They should install bug fix software on their computers.

According to [14], bank customers should avoid surfing the Internet with administrator privileges as this increases their chances of falling prey to the fraudsters. Bank customers should avoid conducting online banking at Internet Cafes; because they do not know how secure the cafe system is. When using the Internet, bank customers should endeavor to activate a browser's security settings to enhance their security online. E-banking services users should endeavor to

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

block Activex Controls and not use a browser's auto-completion function, because it saves information such as the user names and passwords entered while working online [14].

Because some Websites run on cookies, which one must accept to work there, e-banking services users should use security software to prevent these Websites from compiling user information about them. Online banking service users should use browsers that have routers, firewalls, and switches. These features guard the servers and applications against attacks and intrusions [14]. As suggested by [14], customers should ensure their servers have the latest security patches. Internet banking users should do a log file analysis, which can uncover early signs of an attempted break-in before damage is done.

CONCLUSION

Information technology has positively impacted bank productivity and profitability ([9]; 17]). As new development in IT continues to evolve, the delivery of banking products and services continue to take a positive turnaround worldwide. E-banking is a convenient, fast, cost-effective, and time-saving mode of delivery of bank products and services. E-banking enables users to conveniently manage their finances anytime and anywhere; however, electronic transactions can be vulnerable to security threats. According to [13], attacks on e-banking are getting more sophisticated; this makes stronger authentication a necessity. As noted by US CERT, most mobile applications suffer security flaws. [16] stated that 68% of applications do not check server certificates; while 77% ignore SSL errors.

In 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a supplemental guidance to enhance the authentication of Internet banking. Banks are implementing new strategies to educate conservative customers to acquaint them with e-banking usage. [16] suggested that people should refrain from opening unsolicited emails and that banks should update their software periodically to reduce e-banking security threats.

Egbon; wo nori ero o. Oruwo re ni o. (I am not talking about reasoning ability now, you have plenty of that; no doubt about it).

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

REFERENCES

1 Abor J. Technological Innovations and banking in Ghana: An evaluation of Customers' perceptions (2008); Retrieved from www.financialanalyst.org/Technological%20Innovations%20...

2. Bakare S. Varying impacts of electronic banking on the banking industry. Journal of Interrnet Banking and Commerce. 2015; 20(2), 89-98.

3. Boateng R, Molla A. Developing e-banking capabilities lessons. Journal Banking and Commerce. 2006; 11(2), 1-10.

4. Fredrick A. The impact of electronic banking transaction in the banking industry: The case of ADB, SG-SSB and Barclays Bank branches in the eastern region (Master's Thesis). 2012; Available from IDL Dissertation and Theses database. (DCI No. 2013-01-22T10:33:26Z).

5. Foglino J. Threats and challenges for online banking security. n. d.; Retrieved from http://asianbankingandfinance.net/banking-technology/commentary/threats-and-challenges-online-banking-security.

6. Goi C. Sustainability of E-Banking in Malaysia: Opportunities and challenges in the new era. Journal of Internet Banking and Commerce. 2014; 19*(*3), 1-11. Retrieved from http://www.arraydev.com/commerce/jibc/.

7. Guru BK, Vaithilingam S, Ismail N, Prasad R. Electronic banking in Malaysia: A note on evolution of services and consumer reactions. 2004; Retrieved from http://www.researchgate.net.

8 Josefowicz M, Novarica MM. U.S. banking industry trends and IT impacts. 2011; Retrieved from http://www.banktech.com/business-intelligence/us-bankingindustry-trends-and-it-impact/229400115.

9. Keeton WR. The transformation of banking and its impact on consumers and small businesses. Economic Review 1st quarter. 2001; 25-53. Federal Reserve Bank of Kansas City.

10. Kitten T. Phishing attacks on the rise. 2010; Retrieved from http://www.,./ankinfosecurity.com/phishing-attacks-on-rise-a-3080.

11. Kumarjit. The biggest threats to online banking. n. d. ; Retrieved from http://blog.bounceweb.com/the-biggest-security-threats-to-online-banking/.

12. Lee J. Is online banking secure? 5 risks that should worry you. 2015; Retrieved from http://www.makeuseof.com/tag/online-banking-secure-5-recent-breaches-will-worry//.

13. McGlasson L. The top 9 security threats of 2011. 2011; Retrieved from http://www.bankinfosecurity.com/top-9-security-threats-2011-a-3228.

14. Microsoft. Six rules for safer financial transactions online. Retrieved from https://www.microsoft.com/en-us/safety/online-privacy/finances-rules.aspx.

15. Oladejo M, Akanbi T. Bankers' perceptions of electronic banking in Nigeria: A review of post consolidation experience. Research Journal of Finance and Accounting. 2012; 3(2), 1-12.

ISSN: 2455-8834

Volume:02, Issue:07 "July 2017"

16. Paganini P. Cyber criminals, hacktivists, and more: Know your online banking security threats. 2015; Retrieved from https://www.veracode.com/blog/2015/01/cybriminals-hacktivists-and-more-know-your-online-banking-security-threatserc.

17. Papandreou A. Internet banking in Greece: Development, evaluation, and perspectives. 2006; Retrieved from http://www.bth.se/fou/cuppsats.nsf.

18. Shittu O. (2010). The impact of electronic banking in Nigeria banking system: Critical appraisal of Unity Bank PLC.2010.

19. Titrade C, Ciolacu B, Pavel F. E-banking, impact, risks, security. Steconomice. 2008; 4, 1537-1542.

20. Tucker J. The transformation of banking. 2012, Retrieved from http://dailyreckoning.com.

21. Wills T. Mobile Banking: Emerging Threats, Vulnerabilities and Counter-Measures. n. d.; Retrieved from http://www.bankinfosecurity.com.

22. Wueest C. Threats to online banking. n. d.; Retrieved from https://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf.

23. Online banking security. Retrieved from https://fiportal.commerczbank .com/portal/media/fi/.../security/onlinebankingsicherheit.pd.

